



TITLE III Wiretap Overview

Brooklyn Sawyers
Assistant United States Attorney
United States Attorney's Office
Eastern District of Tennessee

What is Title III?

- Title III of the Omnibus Crime Control and Safe Streets Act of 1968
 - Wiretap Act
- Response to the unregulated use of wiretaps
- Congressional scheme for future use
- 18 U.S.C. §§ 2510-2522
- The super search warrant

Title III Administrative Process

- 18 U.S.C. § 2516(1)
- Multi-layered review required
 - Affiant
 - Line AUSA
 - USAO supervisory approval
 - DOJ approval
 - OEO
 - DAAG (see delegation memo)
 - United States District Court approval

Why all the review?

- By way of its statutory scheme, Congress intended not only to limit resort to wiretapping to certain crimes and situations where probable cause is present, but also to condition the use of intercept procedures upon the judgment of a senior official in the Department of Justice that the situation is one of those warranting their use. *United States v. Giordano*, 416 U.S. 505, 527 (1974).

When can Title III be used?

- Investigation must involve predicate offenses
- 18 U.S.C. § 2516
 - Drugs
 - Guns
 - Child Exploitation
 - RICO
 - Money Laundering
 - Health care fraud is not a wire predicate
 - Any federal felony is an electronic predicate

Jurisdiction

- Interception must occur within the court's jurisdiction—18 U.S.C. § 2518(3)
 - Where the facility is located
 - Where the communication signal is redirected (location of switch)
 - Where the communications are first heard or first read

Affidavit Overview

- Federal law enforcement agency
- Affiant qualifications
- Target facility description
- Target subjects/interceptees
- Prior applications
- Probable cause for the target facility
 - CS qualifications and background
- Necessity
- Minimization
- Duration

Probable Cause

- Provide relevant information
- Concise, but include all relevant information
- No lengthy historical information
- Balance providing enough information and omitting information that is not required by statute

Probable Cause

- Department of Justice requirements:
- Six-month rule:
 - Dirty call
 - Transactional
- 21-day rule:
 - Phone record analysis that reveals dirty use of the phone with co-conspirators

Transactional Probable Cause

- Establishes the use of the target phone through phone records surrounding a significant event

Controlled Purchases

- Summarize controlled buys that were arranged over the target phone
 - Remember the controlled buy corroborates the use of the target phone
- Include controlled buy quotes
- Include physical surveillance observations
- Include whether the target phone was used to call the source of supply during the buy

21-Day Rule:

Analysis of Telephone Records

- Toll records or pen register/trap and trace device
- Must have communication in the last 21 days counting backward from the day DOJ approves the request
- Total number of calls (and texts) with each dirty toll hit and the date of the last call (and text)

Necessity

- Purpose is to ensure that wiretapping is not resorted to in situations where traditional investigative techniques would suffice
- Never boilerplate
- Normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous

Necessity

- Confidential Sources
- Controlled Purchases
- Physical Surveillance
- Undercover Agents
- Search Warrants
- Interviews/Grand Jury Subpoenas/Immunity
- Trash Searches

Necessity

- Attempted use of other surveillance techniques
- Pole cameras at locations/residences used by the target subjects
- Tracking devices on vehicles
- Cell site data and/or E-911 information for the target phone and/or other phones used by the target subjects
- Telephone records analysis: pen registers, trap and trace devices, toll analysis and subscriber information
- Mail cover requests
- Other wiretaps
- Financial investigations

Minimization

- Real-time
- 18 U.S.C. § 2518(5)
 - “In the event the intercepted communication is in a code or foreign language, and an expert in that foreign language or code is not reasonably available during the interception period, minimization may be accomplished as soon as practicable after such interception.”
 - Minimization briefing

Duration

18 U.S.C. § 2518(1)(D)

- 30-day period
- 10-day grace period
 - I request that the interception be allowed to continue until all communications which help to fully realize the authorized objectives have been received, or for a period of thirty (30) days, whichever is earlier, and that such period begins on the earlier of the day on which an investigative officer first begins to conduct the interception under the Order, or ten (10) days from the date the Order is entered, pursuant to 18 U.S.C. § 2518(5).

Wiretap Suppression

- Suppression is required under 18 U.S.C. § 2518(10)(a)(i) and (ii) only for “failure to satisfy any of those statutory requirements that directly and substantially implement the congressional intention to limit the use of intercept procedures to those situations clearly calling for the employment of this extraordinary investigative device.” *United States v. Giordano*, 416 U.S. 505, 527 (1974).

Suppression Example: Necessity

- *United States v. Blackmon*, 273 F.3d 1204 (9th Cir. 2001)
- CDCA-controlled substance offenses
- Suppression of wiretap evidence was warranted
- It is inadequate to simply carry over statements from prior applications without making further investigative steps.
- “We hold that the wiretap evidence should be suppressed because the wiretap application contained material misstatements and omissions, and because the application does not otherwise make a particularized showing of necessity.”
 - Common sense approach
 - “It is bereft of specific facts necessary to satisfy the requirements of § 2518(c)(1).”

More Suppression:

United States v. Lomeli, 676 F.3d 734 (8th Cir. 2012)

Suppressed a wiretap for the applicant's failure to identify the designated authorizing DOJ official and attach the AG's memo.

Two issues: Whether the omission of the attached documents was merely a technical defect and whether the *Leon* good-faith exception applied.

Omitting these documents could not be a mere technical defect because correct authorization and proof thereof is the center of the whole statutory scheme limiting the use of intercept procedures to those situations clearly calling for the employment of this extraordinary investigative device. "We hold that no wiretap applicant can, in good faith, rely on a court order authorizing the wiretap when the applicant failed to comply with the edicts of the federal wiretap statute"

United States v. North

- 735 F.3d 212 (5th Cir. 2013)
- Minimization
- Spot monitoring for not more than 2 minutes (absent from appellate record)
- 2518(5) the government's efforts to minimize must be objectively reasonable in light of the circumstances confronting the interceptor
- Listened to non-pertinent conversation (racial profiling) for 1 hour, suspending monitoring only 8 times for less than 1 minute each time

United States v. Glover

- 736 F.3d 509 (D.C. Cir. 2013)
- A judge cannot authorize the interception of communications under statute authorizing wiretaps or electronic bugs if the mobile interception device was not validly authorized, and a device cannot be validly authorized if, at the time the warrant is issued, the property on which the device is to be installed is not located in the authorizing judge's jurisdiction.

QUESTIONS?

THANK YOU